

# **VERMONT STATE AUDITOR'S REPORT ON STATE GOVERNMENT'S PROGRESS TOWARD YEAR 2000 (Y2K) COMPLIANCE**

**FOR THE PERIOD ENDED JUNE 30, 1999**

## **EXECUTIVE SUMMARY**

The State Auditor's Office has conducted this review as a follow-up to its previous reports, released on May 5 and December 31, 1998, concerning the State of Vermont's Y2K compliance efforts. The purpose of this review was to assess the Office of the Chief Information Officer's (CIO) management of the Y2K compliance process and the reliability of its assertions as to the State's overall Y2K preparedness as of the June 30, 1999 compliance deadline set by the Governor.

In our May 1998 report, we found:

- 1. Project management and reporting of compliance status was inadequate.**
- 2. Inadequate centralized leadership resulted in significant gaps in responses by individual offices.**
- 3. Y2K contingency planning was inadequate and misunderstood.**
- 4. Monitoring of State infrastructure that may be affected by non-compliant embedded chips was lacking.**
- 5. Cost estimates for Y2K readiness were undefined.**
- 6. Two key State agencies were "at risk" of not reaching compliance by June 30, 1999.**

In our December 1998 report, we found that there had been significant improvement in centralized management and monitoring of Y2K progress among State agencies and departments by the Office of the CIO. However, weakness were found in the following areas:

- 1. Lack of participation by all State government entities.**
- 2. Lack of a comprehensive computer network inventory of all State systems.**
- 3. Lack of independent verification of assertions made by State agencies that progress had been made.**
- 4. Failure to provide cost estimates for agencies to reach Y2K compliance.**
- 5. Insufficient contingency planning by agency management.**

For the current review period (November 1, 1998 through June 30, 1999), our findings and recommendations are as follows:

**Finding 1.** The Office of the CIO did not have: (1) an accurate list of State entities required by Executive Order #05-99 to participate in the Y2K remediation effort; (2) an information technology (IT) diagram or inventory of State computer systems and linkages; or (3) a definitive inventory of State government mission-critical IT systems. This lack of internal control limited the Office's ability to define the Y2K reporting environment within State government. It also limited the Office's ability to fully identify, analyze and assess the risks to the State from non-compliant IT systems.

While State government appears to have largely complied with the requirement to report Y2K compliance efforts, certain entities have apparently fallen through the cracks. In addition, the Office of the CIO could not provide a definitive list of the 320 mission-critical systems identified by State entities with which to track Y2K reporting.

**Recommendation 1.** In order to provide reasonable assurance about the State's Y2K compliance status, the Office of the CIO should immediately: (1) develop or obtain an accurate list of State entities required by Executive Order #05-99 to participate in the Y2K remediation effort; (2) develop an information technology (IT) diagram or inventory of all State computer systems; and (3) develop a definitive inventory of State government mission-critical IT systems.

-

**Finding 2.** Portions of State government did not report on their Y2K preparedness status. Therefore, the Office of the CIO lacked information and control over the State's Y2K compliance efforts.

Executive Order #05-99 instructed the Office of the CIO to coordinate and oversee the Y2K efforts of "state government agencies, departments, boards and commissions." However, the Board of Medical Practice, the Vermont Center for Geographic Information, the Vermont Economic Development Authority, the Vermont Housing Finance Agency, and the Vermont Veterans' Home (among other State entities) had yet to report their Y2K status to the Office of the CIO by the State's compliance deadline of June 30, 1999.

**Recommendation 2.** The Office of the CIO should require all State boards, commissions, councils, and other executive branch entities to report the status of their Y2K compliance efforts. The Office of the CIO should communicate its broadened authority under Executive Order #05-99 to coordinate and oversee the Y2K activities of these entities.

-

**Finding 3.** The Office of the CIO's guidelines required all State entities that identified themselves as having mission-critical IT systems to submit business contingency plans to the CIO by May 1, 1999. At least seven State entities with

**mission-critical IT systems had not done so by June 30, 1999. These instances of non-compliance increased the risk that State government would not be able to provide critical services in the event of Y2K-related failures.**

The seven State entities that had not submitted Y2K business contingency plans to the Office of the CIO were: Department of Corrections, Office of Economic Opportunity, Enhanced 911 Board, Environmental Board, Judicial Branch, Lottery Commission, and Department of Public Service.

**Recommendation 3. Pursuant to its authority under Executive Order #05-99, the Office of the CIO should require the immediate submission of business contingency plans from all State entities with mission-critical IT systems that have not done so, and request compliance from those entities that are cooperating voluntarily.**

-

**Finding 4. Some contingency plans submitted to the Office of the CIO were non-compliant with State guidelines in that they failed to include required elements such as: (1) a summary of resource needs and costs; (2) identification of the level of services to be provided; and (3) identification of significant dependencies or linkages of the business process with other State entities and external partners.**

Most Y2K business contingency plans submitted to the Office of the CIO complied with State guidelines by specifying alternative means of providing customer services in the event of Y2K-related failures. However, our review raised concerns about the overall integrity of some submissions. Specifically, certain plans failed to meet State guidelines by omitting information about resource needs and costs, the level of services to be provided during a disruption, and significant dependencies or linkages of the business process with other agencies or other partners inside or outside of state government.

**Recommendation 4. In conducting its review of contingency plans, the Office of the CIO should verify that each plan fully discloses significant dependencies or linkages of the business process with other State entities and external partners, and the likelihood of associated Y2K-related failures. The Office of the CIO should request amended contingency plan submissions from those entities that have failed to meet State guidelines.**

-

**Finding 5. The Office of the CIO instructed three State departments – Buildings & General Services, Corrections, and Public Safety – to draft contingency plans that address business continuity in the event that power, heat, and telecommunications are lost. Neither Buildings & General Services nor Public Safety addressed loss of power. Corrections did not submit a contingency plan.**

All but three State entities were instructed to submit contingency plans based on the assumption that power, heat, and telecommunications would be operating normally. Because of the critical nature of the services they provide, the Departments of Buildings & General Services, Corrections, and Public Safety were instructed to address business continuity in the face of such disruptions.

**Recommendation 5. The Office of the CIO should require the Departments of Buildings & General Services, Corrections, and Public Safety to submit contingency plans that provide for business continuity in the event of Y2K-related loss of power, heat, and telecommunications.**

-

**Finding 6. Receipt of a Certificate of Compliance by the Office of the CIO defines a mission-critical IT system as "Y2K compliant." Twenty seven of 41 State entities that identified themselves as having mission-critical IT systems had not filed any Certificates of Compliance for those systems with the Office of the CIO. More than three quarters of the State's mission-critical IT systems were uncertified by the June 30, 1999 deadline.**

The 27 State entities that failed to submit Certificates of Compliance were: Agency of Administration/Office of the CIO, Department of Libraries, Department of Taxes, Agency of Commerce & Community Development, Department of Housing & Community Affairs, Department of Tourism & Marketing, Department of Economic Development, Agency of Human Services (Central Office), Department of Aging & Disabilities, Office of Child Support, Department of Social & Rehabilitation Services, Department of Environmental Conservation, Department of Fish & Wildlife, Department of Forests Parks & Recreation, Department of Motor Vehicles, Attorney General's Office, Department of Banking Insurance Securities and Health Care Administration, Department of Education, Department of Employment & Training, Judicial Branch, Environmental Board, Lottery Commission, Department of Public Service, Secretary of State, Department of States' Attorneys, Department of Corrections, and Legislative Council.

**Recommendation 6. Pursuant to its authority under Executive Order #05-99, the Office of the CIO should require all non-compliant State entities to submit Certificates of Compliance in accordance with the standards outlined in the *Year 2000 (Y2K) Best Practices and Standards Handbook*.**

-

**Finding 7. Because the State's Y2K compliance efforts were measured by inputs ("number of hours worked"), rather than by outcomes ("number of Certificates of Compliance received"), the Office of the CIO could not accurately determine or report the level of State government's Y2K readiness.**

The Office of the CIO based its calculation of overall State Y2K compliance on self reporting of hours spent on Y2K remediation by State entities rather than on the number of Certificates of Compliance received. A weakness of this model was that offices had no incentive to report Y2K compliance deficiencies. Indeed, a recent national survey revealed that state agencies' self-reports of Y2K compliance progress were overly optimistic in their assessment of preparedness status.

**Recommendation 7. The Office of the CIO should measure Y2K compliance by the number of mission-critical IT systems for which it has received Certificates of Compliance signed by agency or department management.**

-

**Finding 8. The Office of the CIO has not independently verified State entities' performance and completion of Y2K work as reported in monthly status reports. As a result, the Office of the CIO lacks assurance about the true level of the State's Y2K compliance.**

Independent verification of State government's Y2K work is especially critical because of the Office of the CIO's use of self-reported data to measure progress toward compliance. A contract to investigate 15-to-20 percent of computer code in eight of the State's 320 mission-critical IT systems does not allow the Office of the CIO to make reliable assertions about overall State Y2K readiness.

**Recommendation 8. In order to maximize the State's preparedness for Y2K-related computer and infrastructure failures, the Office of the CIO should focus on evaluating the integrity of Y2K business contingency plans of all State entities that reported having mission-critical IT systems.**

-

**Finding 9. The Office of the CIO did not have an estimate of the cost of performing the more than 117,000 hours of work reported by 43 State entities in their June 1999 Y2K Project Plans. This lack of information could limit the State's ability to assess the fiscal impact of Y2K compliance activities and to manage its response to emergency requests for Y2K-related funding.**

Nationally, state governments expect to spend more than \$3.5 billion on Y2K activities. According to the National Association of State Information Resource Executives, Vermont is one of seven states failing to identify Y2K costs.

**Recommendation 9. The Office of the CIO should prepare an estimate of the cost of the State's Y2K compliance efforts for legislative consideration in the context of potentially necessary Fiscal Year 2000 supplemental appropriations or Emergency Board outlays.**

## **PURPOSE**

This report is the third in a series of reviews of the State of Vermont's preparedness for and response to the Year 2000 (Y2K) computer date issue during 1998-1999. The purpose of this review was to assess State government's management of the Y2K compliance process and the reliability of its assertions as to the State's overall Y2K preparedness as of the June 30, 1999 compliance deadline set by the Governor.

As we stated in our first report, it is essential that State government provide reasonable assurance that its mission-critical information technology (IT) systems will not be impacted by Y2K problems and that the essential State services upon which Vermonters rely will be maintained in the event of a Y2K-related disruption.

The review was conducted as part of the internal controls segment of the State Auditor's annual audit of the State of Vermont's General Purpose Financial Statements. It applied standards consistent with the Statement on Auditing Standards No. 78, issued by the American Institute of Certified Public Accountants.

## **SCOPE**

The Vermont State Auditor's third Y2K report:

1. Follows up on the issues identified in previous Y2K review reports released on May 5, 1998 and December 31, 1998;
2. Assesses the reliability of the State's reported Y2K status as of the compliance deadline established by Executive Orders #11-98 and #05-99 (June 30, 1999) for mission-critical IT systems;
3. Assesses the State's Y2K compliance in terms of contingency planning activities and results.

The Office of the Chief Information Officer (CIO) has been directly charged by the Governor with ensuring Y2K compliance throughout State government. The management and monitoring of the State's Y2K efforts by the Office of the CIO was critical to the State's success or failure in meeting the goal of compliance by June 30, 1999. The Auditor's review has focused on internal controls and compliance by the Office of the CIO with regard to Vermont Statutes Annotated (V.S.A.), Title 3, Sections 2222(a)(9) and (10), delegating responsibility for planning the State's short-and long-term information technology strategies.

It assessed the reliability of the Office of the CIO's estimate of State government's Y2K compliance status as well as the Office of the CIO's overall management of the State's

Y2K compliance efforts during the eight-month assessment period (November 1, 1998 to June 30, 1999).

## **AUTHORITY**

This review was conducted pursuant to the State Auditor's authority contained in 32 V.S.A. §§ 163 and 167.

## **METHODOLOGY**

This review of the State's Y2K compliance activities (as of June 30, 1999) was conducted from November 1, 1998 through September 1, 1999.

Our methodology included:

1. Review of Executive Orders 11-98 and 05-99.
2. Review of the CIO's *Year 2000 [Y2K] Best Practices and Standards Handbook*.
3. Review of the CIO's *Y2K Contingency Plan Guidelines*.
4. Review of monthly Y2K Project Plans and Status Reports submitted by government agencies for the months July 1998 through June 1999.
5. Review of Vermont Agency of Administration's response to individual agencies regarding their Y2K Status Reports and action steps necessary to stay on schedule.
6. Interviews with the Secretary of Administration, CIO and assistant CIO (Y2K Coordinator).
7. Conversations with information technology directors/administrators from key State offices.
8. Attendance at the Office of the CIO's monthly Y2K workshops.
9. Review of the CIO's published information technology policies.
10. Review of the State's Information Technology Five-Year Plan.
11. Review of various General Accounting Office (GAO) guides and reports. (The CIO has adopted GAO's format for addressing Y2K issues in State government.)
12. Review of State Y2K reports as well as GAO and federal Office of Management and Budget (OMB) reports.
13. Results of GAO survey completed by State offices that significantly interface with the federal government.
14. Review of Year 2000 compliance efforts undertaken by the federal government and selected state and local governments.
15. Review of news articles relating to Y2K issues and global impact on public and economy.
16. Survey of selected Web sites focusing on Y2K standards and experiences.

To evaluate the State's progress toward Y2K compliance, the SAO adopted the problem-solving approach suggested by the Gartner Group, an internationally regarded information technology consulting firm, and OMB.

## **BACKGROUND**

### **A. WHAT IS "Y2K"?**

The Y2K problem is caused by computers and information technology systems that utilize two digits to represent the year. As the year 2000 arrives, there is a danger that non-compliant systems may think it is the year 1900 rather than 2000, and may not work properly or may shut down completely. Fundamentally, then, Y2K is a time-sensitive issue. Likewise, auditing is a time-sensitive process. Audit work is generally performed in a retrospective manner, assessing financial practices and procedures, compliance and internal controls during a specified period of time. Following professional standards, this report cannot report on the State's Y2K compliance activities as of today. It does, however, assess the State's Y2K compliance activities as of June 30, 1999 – the deadline established by executive order by which the State of Vermont would be Y2K-compliant. The State's current Y2K preparedness may or may not be similar to what we measured during the period of this review.

### **B. DUTIES AND RESPONSIBILITIES OF THE CHIEF INFORMATION OFFICER (CIO)**

The Office of the CIO is charged with ensuring Y2K compliance throughout State government. The management of the State's Y2K efforts is critical to the success or failure of the State to meet established compliance goals.

The CIO reports directly to the Secretary of Administration. The CIO's Y2K responsibilities include:

1. Coordinating and overseeing Y2K efforts throughout State government to ensure consistent and timely reporting and compliance efforts;
2. Providing support to each department (and each manager), through:
  - a. Y2K processes and standards,
  - b. Specialized contracts and legal support,
  - c. Creation and maintenance of a Web site for Y2K reporting, tools and vendor compliance information [<http://y2k.state.vt.us/y2k/>],
  - d. Contingency planning guidance,
  - e. Assistance with special projects;
3. Centralized tracking of Y2K progress;
4. Reporting progress to the Secretary of Administration, Legislature and other external audiences;

5. Acting as spokesperson regarding Y2K efforts for the State of Vermont.

## **C. PREVIOUS REPORTS**

This report is the third in a series of Y2K reviews by the Vermont State Auditor's Office. Findings from our prior two reviews are summarized below.

### ***MAY 5, 1998 REPORT (FOR THE PERIOD ENDED APRIL 1, 1998)***

The SAO initially reviewed the State's Y2K compliance activities as of April 1, 1998 and released a status report on May 5, 1998. Initial findings were:

1. **Project management and reporting of compliance status was inadequate.**
2. **Inadequate centralized leadership resulted in significant gaps in responses by individual offices.**
3. **Y2K contingency planning was inadequate and misunderstood.**
4. **Monitoring of State infrastructure that may be affected by non-compliant embedded chips was lacking.**
5. **Cost estimates for Y2K readiness were undefined.**
6. **Two key State agencies were "at risk" of not reaching compliance by June 30, 1999.**

### ***DECEMBER 31, 1998 REPORT (FOR THE PERIOD ENDED NOVEMBER 1, 1998)***

The second status report, published on December 31, 1998, showed significant improvement in the management and monitoring of Y2K progress among State agencies by the Office of the CIO. Weaknesses were found in the following areas:

1. **Lack of participation by all State government entities.**
2. **Lack of a comprehensive computer network inventory of all State systems.**
3. **Lack of independent verification of assertions made by State agencies that progress had been made.**
4. **Failure to provide cost estimates for agencies to reach Y2K compliance.**
5. **Insufficient contingency planning by agency management.**

## **FINDINGS AND RECOMMENDATIONS**

### **Risk Assessment**

#### **Finding 1**

**The Office of the CIO did not have:**

1. **An accurate list of State entities required by Executive Order #05-99 to participate in the Y2K remediation effort;**
2. **An information technology (IT) diagram or inventory of State computer systems and linkages;**
3. **A definitive inventory of State government mission-critical IT systems.**

**This lack of internal control limited the Office's ability to define the Y2K reporting environment within State government. It also limited the Office's ability to fully identify, analyze and assess the risks to the State from non-compliant IT systems.**

### Discussion

The Office of the CIO is responsible for providing support and guidance to State managers to ensure Y2K compliance throughout State government. Part of this responsibility includes the ability to appropriately assess progress and report on the State's readiness to the Secretary of Administration, the Legislature, Vermont citizens and other external audiences.

Most State agencies and departments have designated a specific individual to serve as the official Y2K contact person and in-house project manager. Each participating Y2K representative received a State of Vermont Organization Chart from the Office of the CIO, and was asked to contact all State offices associated with their respective agency and obtain written documentation attesting to general Y2K readiness and compliance of mission-critical IT systems. These certifications were to be used to determine the Y2K compliance of each State agency or department, to identify potential risks to business continuity, and possibly to help inform broader emergency planning efforts.

Although the State organizational chart is helpful, it does not represent a comprehensive and accurate list with which the Office of the CIO can verify that all areas of State government below the agency and department levels have been included in the State's decentralized Y2K efforts. The absence of such a basic management tool prevents the Office of the CIO from providing the highest degree of assurance about overall Y2K readiness. Without it, the Office of the CIO cannot verify that it has received comprehensive status reports from all State offices, inventoried all mission-critical areas and completely assessed risks and verified contingency plans.

While State government appears to have largely complied with the requirement to report Y2K compliance efforts (per Executive Order 05-99), certain entities have apparently fallen through the cracks [see discussion, Finding 2]. Due to the absence of an accurate master list of State entities, the Office of the CIO cannot confirm universal participation throughout State government or by all sections of any given State agency or department.

Similarly, the absence of a comprehensive diagram or inventory of State government's computer systems and their linkages weakens the Office of the CIO's ability to provide assurances about Y2K compliance. If reporting entities omit IT components from their Y2K reporting, the Office of the CIO does not have a template against which to confirm

that assessments have been completed for all systems. Without an IT architectural diagram or inventory, the State runs the risk that, even if all mission-critical IT systems are checked, these systems could be endangered by smaller IT components that have not been checked, or through linkages with the State's external electronic partners. Executive Order #05-99 specifically states that "the date on which all mission-critical IT systems should be brought into Year 2000 compliance is June 30, 1999." The inability to define or delineate systems unique to each department or agency means that the Office of the CIO cannot provide assurance that all critical systems were in compliance by June 30 or at any time thereafter. And while agencies and departments have been instructed by the Office of the CIO to assess every interface area, they have not been required to provide documentation of the Y2K readiness of electronic linkages with external partners in their monthly status reports.

Since our December 1998 Y2K report, some progress has been made with respect to the State's electronic interfaces with the federal government. In conjunction with the federal General Services Administration, the Office of the CIO has compiled a list of State computer systems that exchange data with the federal government. Due to inconsistent reporting methods between states and the federal government, the GSA's Federal-State Data Exchange was discontinued in April, 1999. Nonetheless, it is important that the Office of the CIO analyze the list to determine whether Vermont State government is aware of and working with federal counterparts to ensure that these interfaces are ready for the Year 2000.

Monthly Y2K Project Plans submitted to the Office of the CIO by 43 Vermont State government entities indicate that there are approximately 320 systems considered mission-critical by these agencies. Information submitted by the CIO on April 21, 1999 to the National Association of State Information Resource Executives' (NASIRE) Year 2000 Remediation Results Survey, however, indicated that the State of Vermont had only 80 mission-critical IT systems. There is an obvious discrepancy in the number of mission-critical IT systems identified by State agencies and departments and that reported by the CIO to NASIRE.

State entities are required to submit Certificates of Compliance for each mission-critical IT system to the Office of the CIO [see Finding 6]. The Office of the CIO could not provide a definitive list of the 320 mission-critical IT systems identified by State entities (or the list of the 80 systems reported to NASIRE) with which to track Y2K reporting. Without an exact inventory of mission-critical IT systems, the Office of the CIO might experience difficulty in tracking the receipt of Certificates of Compliance and following up with State entities that had yet to file. Indeed, the Office of the CIO would have needed such a list to determine which mission-critical IT systems were non-compliant as of June 30, 1999 and to accurately measure the overall level of the State's Y2K readiness.

### **Recommendation 1**

**In order to provide reasonable assurance about the State's Y2K compliance status, the Office of the CIO should immediately:**

1. **Develop or obtain an accurate list of State entities required by Executive Order #05-99 to participate in the Y2K remediation effort;**
2. **Develop an information technology (IT) diagram or inventory of all State computer systems;**
3. **Develop a definitive inventory of State government mission-critical IT systems.**

-

## **Finding 2**

**Portions of State government did not report on their Y2K preparedness status. Therefore, the Office of the CIO lacked information and control over the State's Y2K compliance efforts.**

### **Discussion**

The State Auditor's December 1998 Y2K report found that certain areas of State government had not communicated with the Office of the CIO about Y2K compliance efforts. Executive Order #11-98, then in effect, instructed the Office of the CIO to "coordinate and oversee the State's Year 2000 efforts," and ordered "agencies and departments" to report on their Y2K compliance efforts. The CIO, in a formal response to the Auditor's December report, indicated that the Governor would be requested to amend his Executive Order to instruct boards and commissions to report their compliance efforts as well.

The amended Executive Order (#05-99) was issued on May 11, 1999. It instructed the Office of the CIO to coordinate and oversee the Y2K efforts of "state government agencies, departments, boards and commissions," but did not specifically require or encourage boards, commissions and other executive branch entities to report Y2K compliance efforts to the Office of the CIO.

As a result, the following State entities (among others) had yet to report their Y2K status to the Office of the CIO by the State's compliance deadline of June 30, 1999:

1. Board of Medical Practice
2. Vermont Center for Geographic Information
3. Vermont Economic Development Authority
4. Vermont Housing Finance Agency
5. Vermont Veterans' Home

There are approximately 150 State boards, councils, commissions and committees within Vermont State government. While some of these organizations may lack a physical office and may have no equipment, there is no way for the Office of the CIO to determine their status unless they report. All entities should be required (or, if outside the authority of an executive order, encouraged) to report to the Office of the CIO in order to confirm the

level of their Y2K readiness, so that the Office of the CIO is fully informed about Y2K compliance throughout State government.

## **Recommendation 2**

**The Office of the CIO should require all State boards, commissions, councils, and other executive branch entities to report the status of their Y2K compliance efforts. The Office of the CIO should communicate its broadened authority under Executive Order #05-99 to coordinate and oversee the Y2K activities of these entities.**

-

## **Contingency Plans**

### **Finding 3**

**The Office of the CIO's guidelines required all State entities that identified themselves as having mission-critical IT systems to submit business contingency plans to the CIO by May 1, 1999. At least seven State entities with mission-critical IT systems had not done so by June 30, 1999. These instances of non-compliance increased the risk that State government would not be able to provide critical services in the event of Y2K-related failures.**

### **Discussion**

The Secretary of Administration instructed individual State entities to develop contingency plans for mission-critical IT systems.

The CIO's *Y2K Business Contingency Plan Guidelines* instructed State entities to submit business contingency plans by May 1, 1999. At the end of the audit period, which coincided with the State's Y2K compliance deadline of June 30, 1999, the following State entities that identified themselves as having mission-critical IT systems had not submitted business contingency plans to the Office of the CIO:

1. Department of Corrections
2. Office of Economic Opportunity
3. Enhanced 911 Board
4. Environmental Board
5. Judicial Branch
6. Lottery Commission
7. Department of Public Service

Some entities that had yet to report to the Office of the CIO may have mission-critical IT systems. Among these were:

1. Board of Medical Practice

2. Criminal Justice Training Council
3. Human Rights Commission
4. Vermont Center for Geographic Information
5. Vermont Economic Development Authority
6. Vermont Housing Finance Agency
7. Vermont Veterans' Home

### **Recommendation 3**

**Pursuant to its authority under Executive Order #05-99, the Office of the CIO should require the immediate submission of business contingency plans from all State entities with mission-critical IT systems that have not done so, and request compliance from those entities that are cooperating voluntarily.**

-

### **Finding 4**

**Some contingency plans submitted to the Office of the CIO were non-compliant with State guidelines in that they failed to include required elements such as:**

- 1. A summary of resource needs and costs,**
- 2. Identification of the level of services to be provided, and**
- 3. Identification of significant dependencies or linkages of the business process with other State entities and external partners.**

### **Discussion**

The CIO's *Y2K Contingency Plan Guidelines* instructed State entities to draft contingency plans that would provide continuity in business functions in the event of a disruption to normal business operations. These guidelines provide Vermont State agencies and departments with specific guidance in developing comprehensive, useable contingency plans. At a minimum, the guidelines require that each reporting entity's contingency plan address all mission-critical business functions (including those handled by outside parties) and provide an overall summary of resource needs and costs to put the plans into effect for all identified business functions. Specifically, for each business process covered by the contingency plan, reporting entities are instructed to provide information about the following:

1. A brief overview of the process,
2. A diagram of the process,
3. All significant dependencies or linkages with other State agencies or external partners,
4. The nature and likelihood of any expected Y2K-related disruptions,
5. The major assumptions inherent in the plan,
6. All specific events and conditions that would trigger the plan,

7. The level of services to be provided during the disruption,
8. The expected life cycle or duration of the plan,
9. The procedures to be followed for dealing with specific, identified events,
10. A summary of detailed, step-by-step procedures for initiating and executing contingency operations, and for transitioning back to normal operations,
11. A list of names and contact information for employees needed to execute the plan,
12. A description of necessary testing of the plan,
13. Any significant resources necessary to implement the plan.

The Office of the CIO has adopted the U.S. General Accounting Office's (GAO) business continuity and contingency plan guidelines as its standard. The GAO instructed that a well-developed contingency plan "safeguards an agency's ability to produce *a minimum acceptable level of outputs and services* [emphasis added] in the event of failures of internal or external mission-critical information systems and services." It outlined four major steps in the development of a Y2K business contingency plan:

1. *Initiation* – Establish a business continuity project work group and develop a high-level business continuity planning strategy. Develop master schedules and milestones, and obtain executive support.
2. *Business Impact Analysis* – Assess the potential impact of mission-critical system failures on core business processes. Define Y2K failure scenarios, and perform risk and impact analyses of each core business process. Assess infrastructure risks, and define the minimum acceptable levels of outputs for each core business process.
3. *Contingency Planning* – Identify and document contingency plans and implementation modes. Define triggers for activating contingency plans, and establish a business resumption team for each core business process.
4. *Testing* – Validate the business continuity strategy. Develop and document contingency test plans. Prepare and execute tests. Update disaster recovery plans and procedures.

Most Y2K business contingency plans submitted to the Office of the CIO complied with State guidelines by specifying alternative means of providing customer services in the event of Y2K-related failures. However, our review raised concerns about the overall integrity of some submissions. Certain plans failed to include important elements required by State guidelines. Here are some examples:

1. State Standard: *Contingency plans should provide an overall summary of resource needs and costs.*

Compliance: The Department of Banking, Insurance, Securities and Health Care Administration, responsible for regulating the industries enumerated in its title, submitted a contingency plan that outlined specific costs associated with hiring temporary workers, renting portable generators, and obtaining manual typewriters.

Non-compliance: The Department of Finance and Management, Financial Operations Division, responsible for operating the State's Financial Management Information System (FMIS), submitted a contingency plan that included no cost estimates for manually processing checks. It also did not estimate the cost of overtime pay for staff who will work during the weekend of January 1-2, 2000 to balance month-end financial reports.

2. State Standard: *Contingency plans should describe the level of services to be provided during the disruption.*

Compliance: The Department of Employment and Training, which provides unemployment benefits to out-of-work Vermonters, submitted a contingency plan that identified 17 separate business functions and provided strategies to ensure that the Department's mission (including the processing of unemployment claims) would be fulfilled in the event of Y2K-related system failures.

Non-compliance: The Department of Developmental and Mental Health Services, which provides services to vulnerable adults and children and manages the Vermont State Hospital (VSH), submitted a two-page contingency plan that did not address how Medicaid payments would be made in the event of computer failures and did not address the provision of services to VSH patients (apart from making basic provisions to have extra supplies on hand).

3. State Standard: *Contingency plans should describe any significant dependencies or linkages of the business process with other agencies or other partners inside or outside of State government.*

Compliance: The Agency of Transportation (AOT), responsible for keeping State highways clear of ice and snow for both emergency vehicles and the general public, submitted a contingency plan that addressed the possibility of fuel delivery problems. AOT's plan includes preparations to top off fuel storage tanks at all of its garages in the two weeks prior to January 1, 2000.

Non-compliance: The Department of Public Safety, charged with the responsibility of providing on-call emergency services to the general public, submitted a contingency plan that did not address fuel availability for department vehicles in the event of a disruption.

While Vermont's contingency planning guidelines seem to largely encompass the standards adopted from the GAO, it is important to know how individual plans were created and whether agency and department management was involved in the process. The GAO instructs that an effective Y2K contingency planning approach is collaborative. It recommends establishing a business continuity work group, with support from management, to work in collaboration with the Y2K project manager. In its contingency plan, for example, the Department of Buildings & General Services listed the members of

its Y2K contingency planning team, including the specific roles each played in the planning process.

This team approach underscores the fact that contingency planning is not just about information technology fixes, but should result in the production of a road map that the government entity can use to provide mission-critical services in the face of Y2K-related failures. In reviewing contingency plan submissions, the Office of the CIO should verify that this GAO standard was heeded. If a Y2K project manager single-handedly authored a Y2K business contingency plan without assistance from management or a Y2K work group, there is a danger that core business functions may have been omitted. The Office of the CIO has no way of verifying such omissions directly, as individual agencies and departments are relied upon to provide the list of critical functions, but the Office can review the process that was followed to formulate each plan.

The deadline for Y2K compliance arrived on June 30, 1999. State government should use the time remaining before the year 2000 to continue to prepare for Y2K-related impacts. Contingency planning is an element of the Y2K remediation process that the Office of the CIO should spend time reviewing closely during the remaining months of 1999.

#### **Recommendation 4**

**In conducting its review of contingency plans, the Office of the CIO should verify that each plan fully discloses significant dependencies or linkages of the business process with other State entities and external partners, and the likelihood of associated Y2K-related failures. The Office of the CIO should request amended contingency plan submissions from those entities that have failed to meet State guidelines.**

-

#### **Finding 5**

**The Office of the CIO instructed three State departments – Buildings & General Services, Corrections, and Public Safety -- to draft contingency plans that address business continuity in the event that power, heat, and telecommunications are lost. Neither Buildings & General Services nor Public Safety addressed loss of power. Corrections did not submit a contingency plan.**

#### **Discussion**

With the exception of three agencies, the Office of the CIO instructed all agencies to submit contingency plans based on the assumption that all buildings would have power, telephones, heat, and voice and data communications. The Departments of Buildings & General Services, Corrections, and Public Safety were each required to submit contingency plans that addressed business continuity in the event of electrical, heat, and telecommunications breakdowns on or around January 1, 2000. Two of these three

departments (Buildings & General Services, and Public Safety) did not provide contingencies for business continuity in the event of a power failure, and the third (Corrections) had not filed a contingency plan by June 30, 1999.

The Department of Buildings & General Services is responsible for ensuring that all State government buildings and infrastructure will be fully functional at the turn of the century. The contingency plan for that department assumes that "public utilities and voice and data communications will be functioning in a normal manner supplying services to all sites." That does not comply with the directive issued by the Office of the CIO.

The Department of Public Safety is responsible for the detection and prevention of crime generally, participation in the search and rescue of lost or missing persons, and assistance in statewide or local disasters or emergencies. By failing to identify alternative power sources in its contingency plan, it did not comply with the Office of the CIO's directive.

The Department of Corrections, responsible for managing correctional facilities designed to house criminal offenders, failed to meet the CIO's May 1, 1999 contingency plan submission deadline. It also had failed to file a plan by the State's June 30, 1999 Y2K compliance deadline.

Although not required by the Office of the CIO, contingency plans submitted by the Department of Banking, Insurance, Securities and Health Care Administration (BISHCA), the Department of Employment and Training (DET), and the Department of Social and Rehabilitation Services (SRS) addressed business continuity in the event of infrastructure failures. BISHCA and DET provided alternative strategies for dealing with utility disruptions. SRS included alternative security, food and communication strategies.

### **Recommendation 5**

**The Office of the CIO should require the Departments of Buildings & General Services, Corrections and Public Safety to submit contingency plans that provide for business continuity in the event of Y2K-related loss of power, heat, and telecommunications.**

## **Y2K Compliance**

### **Finding 6**

**Receipt of a Certificate of Compliance by the Office of the CIO defines a mission-critical IT system as "Y2K compliant." Twenty seven of 41 State entities that identified themselves as having mission-critical IT systems had not filed any Certificates of Compliance for those systems with the Office of the CIO. More than three quarters of the State's mission-critical IT systems were uncertified by the June 30, 1999 deadline.**

## Discussion

The purpose of the Certificate of Year 2000 Compliance is to formally certify that a computer system has received any necessary renovation in accordance with the requirements of the Y2K repair process and is officially "Y2K compliant." Receipt of these signed Certificates indicates to the Office of the CIO that the system meets the standard for compliance and that appropriate agency staff has verified and approved the end product.

Of the 46 government entities that had submitted monthly Y2K Project Plans and Status Reports to the Office of the CIO, 43 reported having 320 mission-critical IT systems. [See [Table 1.](#)]

A total of 170 Certificates of Compliance were submitted by 14 of the 41 State entities that had identified mission-critical IT systems for which they are responsible. [See Table 2.] The 27 entities that failed to submit certificates by the June 30, 1999 deadline were:

1. Agency of Administration/Office of the CIO
2. Department of Libraries
3. Department of Taxes
4. Agency of Commerce & Community Development
5. Department of Housing & Community Affairs
6. Department of Tourism & Marketing
7. Department of Economic Development
8. Agency of Human Services, Central Office
9. Department of Aging & Disabilities
10. Office of Child Support
11. Department of Social & Rehabilitation Services
12. Department of Environmental Conservation
13. Department of Fish & Wildlife
14. Department of Forests, Parks & Recreation
15. Department of Motor Vehicles
16. Attorney General's Office
17. Department of Banking, Insurance, Securities and Health Care Administration
18. Department of Education
19. Department of Employment & Training
20. Judicial Branch
21. Environmental Board
22. Lottery Commission
23. Department of Public Service
24. Secretary of State
25. States' Attorneys
26. Department of Corrections
27. Legislative Council

## **Recommendation 6**

**Pursuant to its authority under Executive Order #05-99, the Office of the CIO should require all non-compliant State entities to submit Certificates of Compliance in accordance with the standards outlined in the *Year 2000 (Y2K) Best Practices and Standards Handbook*.**

### **Finding 7**

**Because the State's Y2K compliance efforts were measured by inputs ("number of hours worked"), rather than by outcomes ("number of Certificates of Compliance received"), the Office of the CIO could not accurately determine or report the level of State government's Y2K readiness.**

### **Discussion**

The formula used by the Office of the CIO to determine each State entity's progress toward Y2K preparedness was *the estimated number of hours required to complete each phase* (awareness, assessment, renovation, validation, implementation) *of the Y2K compliance effort divided by the number of hours actually completed*. A Y2K Project Plan and Status Report detailing the completed number of hours was submitted monthly by each entity, but was not subject to independent verification. Furthermore, initial estimates of the number of hours required to complete each phase of the Y2K effort were sometimes revised upwards or downwards by individual State entities.

The weakness of the Office of the CIO's self-reporting model was that offices had no incentive to report Y2K compliance deficiencies. Reporting of Y2K status measured only how far along an office was in relation to its own internal hourly budget estimate. There may have been a tendency for offices to understate the scope of Y2K compliance problems, and since the Office of the CIO did not assess these reports, such underestimation could easily have gone undetected. There may also have been a tendency for offices to overstate their effort, which could similarly have gone undetected. Indeed, a recent survey of 27 states' Y2K compliance efforts by the National State Auditors' Association revealed that State agencies' self-reporting of Y2K compliance progress was overly optimistic in their assessment of preparedness status.

The Office of the CIO based its calculation of overall State Y2K compliance on these self reports rather than on the number of Certificates of Compliance received. An examination of nine other states' Y2K progress reports did not reveal the type of quantitative measure Vermont has used to assess Y2K compliance. Instead, several states track the number of mission-critical IT systems per agency and ask these agencies to report the number of Y2K-compliant systems. These states then obtain a "percent complete" value by dividing number of systems in compliance by total number of systems. The Office of the CIO's use of this *input* measure ("number of hours worked"), rather than an *outcome* measure ("number of Certificates of Compliance received"), to

assess progress and to rate agency readiness was a fundamental weakness in its overall project management of the Y2K remediation effort.

Particularly now that the June 30, 1999 Y2K compliance deadline has passed, the only measure that has real meaning is actual Y2K compliance of mission-critical IT systems. State standards clearly define a "Y2K-compliant" system as one for which the Office of the CIO has received a Certificate of Compliance.

### **Recommendation 7**

**The Office of the CIO should measure Y2K compliance by the number of mission-critical IT systems for which it has received Certificates of Compliance signed by agency or department management.**

### **Finding 8**

**The Office of the CIO has not independently verified State entities' performance and completion of Y2K work as reported in monthly status reports. As a result, the Office of the CIO lacks assurance about the true level of the State's Y2K compliance.**

### **Discussion**

The December 1998 Y2K review issued by the State Auditor's Office recommended that the Office of the CIO engage the services of an independent contractor to verify the Y2K efforts reported in monthly status reports by State entities. These reports document the number of hours completed out of an estimated total required to complete the five phases of the Y2K remediation effort – awareness, assessment, renovation, validation, and implementation.

The Office of the CIO issued a Request for Proposal (RFP) to Perform Year 2000 Independent Validation of mission-critical IT systems. When all responding bidders proposed contracts in excess of the \$200,000 appropriation for the contract in the Fiscal Year 1999 Budget Adjustment Act, the scope of the RFP was narrowed and bids again were sought. The contract, finalized after the end of the review period for this report, was for a plan to spot check 15-to-20 percent of computer code and review system and testing documentation in eight mission-critical IT systems. The original plan was to verify 100 percent of the code and associated documentation in the State's mission-critical IT systems. Independent validation of infrastructure in 1,700 State buildings was removed from the plan as well.

Independent verification of State government's Y2K work is especially critical because of the Office of the CIO's use of self-reported data to measure progress toward compliance. Without some sort of verification by management, there can be no assurance

that the reported number of hours were actually spent on Y2K remediation or that the work actually resulted in Y2K-compliant IT systems. Confirmation of code remediation alone, without an investigation of the integrity of contingency plans and the Y2K status of electronic partners, is not sufficient to verify overall Y2K compliance.

The Office of the CIO cannot make reliable assertions about overall State Y2K readiness based on an investigation of 15-to-20 percent of computer code and supporting documentation for eight of 320 mission-critical IT systems, at six of 46 reporting State entities. Ideally, there would be more time and more resources available to broaden the scope of the contract, but given the lack of assurance about State government's Y2K compliance at the project completion deadline, it would be in the better interest of the State to increase preparedness for Y2K-related computer and infrastructure failures by verifying the integrity of business contingency plans.

### **Recommendation 8**

**In order to maximize the State's preparedness for Y2K-related computer and infrastructure failures, the Office of the CIO should focus on evaluating the integrity of Y2K business contingency plans of all State entities that reported having mission-critical IT systems.**

### **Cost**

### **Finding 9**

**The Office of the CIO did not have an estimate of the cost of performing the more than 117,000 hours of work reported by 43 State entities in their June 1999 Y2K Project Plans. This lack of information could limit the State's ability to assess the fiscal impact of Y2K compliance activities and to manage its response to emergency requests for Y2K-related funding.**

### **Discussion**

A critical element of the Office of the CIO's Y2K management should be the ability to provide necessary information to the Legislature and other parties about the State's Y2K expenditures. As first noted in Vermont State Auditor's Report issued December 31, 1998, the Office of the CIO cannot provide an estimate of the financial costs associated with State Y2K compliance efforts. Apart from a handful of specified Y2K-related expenditures in the Fiscal Year 1999 supplemental budget, the extent to which the State budget or normal operational goals have been impacted is undisclosed.

Nationally, state governments expect to spend more than \$3.5 billion on Y2K activities (as estimated on July 29, 1999). Information from a report dated May 18, 1999, and the

most current information available from NASIRE's Survey of the States, indicates that Vermont is one of seven states failing to identify Y2K costs.

### **Recommendation 9**

**The Office of the CIO should prepare an estimate of the cost of the State's Y2K compliance efforts for legislative consideration in the context of potentially necessary Fiscal Year 2000 supplemental appropriations or Emergency Board outlays.**